TAKING ACTION:

Identity Theft Victim Recovery Checklist

The scope of identity theft often goes beyond an unauthorized credit card charge. Whether it is tax-related, child identity theft, or medical identity theft, **identity theft is a crime, and it can be devastating.** When your personal information has been stolen, you may be coping with the aftermath of a compromised identity, damaged credit, and financial loss, as well as a painful range of emotions including anger, fear, and frustration.

It is critical that you take immediate steps to stop and repair the damage caused by identity theft. Reporting the crime, no matter how small, helps law enforcement, regulators, and government agencies put a stop to the fraud, prevent the victimization of more consumers, and pursue the criminals.

Very often, perpetrators will dispose of your money immediately after taking it. You may never get your money back. That said, your recovery is about more than lost money. It is about taking steps to minimize the harm, protect your future financial health and assets, and recover emotionally from the crime.

We recommend taking the steps below to reclaim power from the fraudsters and help you move forward.

CREDIT CARD IDENTITY THEFT

The typical case of identity theft involves stolen credit cards or unauthorized charges on your credit card. If your credit card number was stolen or used fraudulently, you should:

- Contact the relevant banks or credit card companies to notify them of the theft and dispute fraudulent charges; and
- Carefully read account statements regularly to look for fraudulent charges.

NATIONAL CENTER FOR VICTIMS OF CRIME

FINRA Investor Education FOUNDATION

Credit card abuse may be a sign that your identity has been compromised more broadly beyond a single account. Be alert to suspicious activity in your other financial accounts or credit reports, which could indicate that the theft extends well beyond your credit card. **If you spot unusual activity in any of your accounts or are a victim of identity theft unrelated to your credit card, you will need to take the following steps.**

STEP 1 – Place a Fraud Alert*

You will need to place a fraud alert with one of the three credit reporting companies to be notified of any new requests for credit. If not authorized by you, these credit requests may be indications of widespread identity theft:

- contact one of the three credit reporting companies (Equifax, Experian, or TransUnion);
- tell the company you are a victim of identity theft and request that a fraud alert be placed on your credit report (this initial fraud alert will last for 90 days);
- ask the company to report this request to the other two credit reporting companies; and
- order your free credit report; by creating the fraud alert, you are entitled to one free copy from each credit reporting company within 12 months of placing the alert, regardless of when you reqested your last report.

FREE CREDIT REPORT

AnnualCreditReport.com is the only official source for free credit reports. All consumers, regardless of a fraud alert, are entitled to receive one free credit report every 12 months from each of the following companies:

EQUIFAX
(800) 685-1111
www.equifax.com

EXPERIAN
(888) 397-3742
www.experian.com

TRANSUNION
(800) 916-8800
www.transunion.com

STEP 2 – Create an Identity Theft File

Collect all relevant documentation concerning the theft in one file that is kept in a secure location. The file should include:

- a timeline of events, which may span many years;
- the police report, if any;
- the identity theft affidavit (see Step 4);
- your most recent credit report from all three credit reporting companies;
- your Internal Revenue Service identity theft affidavit (see Step 8);

*Adapted from the Federal Trade Commission's "Taking Charge: What to Do If Your Identity Is Stolen," downloadable at www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf. Order hard copies online at https://bulkorder.ftc.gov/ShowCat.aspx?s=idt-04.

- any evidence of the identity theft, including any information about the perpetrator;
- all written or email communication with creditors, banks, financial institutions, or credit reporting companies; and
- logs of any phone conversations, with dates, names, and phone numbers of any representatives with whom you spoke, and notes on what information they gave you.

STEP 3 – Know Your Rights

You have rights created by federal and, in some cases, state law. Learn about your rights to better protect yourself.

- For federal victim rights, you can review the Federal Trade Commission's information at www.identitytheft.gov/know-your-rights.
- For state victim rights, check with your state attorney general, whose contact information is available at www.naag.org.
- For additional information and resources, visit the Identity Theft Resource Center at www.idtheftcenter.org or call (888) 400-5530 (open 24/7).

FTC IDENTITY THEFT GUIDE

IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. Hosted by the FTC, this site is an additional source of checklists and sample letters to guide you through the recovery process.

ENGLISH

www.identitytheft.gov

SPANISH

www.robodeidentidad.gov

STEP 4 – Report the Identity Theft to the Federal Trade Commission and Build a Recovery Plan at IdentityTheft.gov

Lodging a complaint with the Federal Trade Commission, using the FTC's complaint assistant, will also enter the fraud into the Consumer Sentinel Network so that law enforcement can stop ongoing fraud and track these crimes. *This process will not initiate a criminal investigation of your case.*

Federal Trade Commission Complaint Assistant
www.ftccomplaintassistant.gov

- After completing the complaint process, print the identity theft affidavit created by the completion of the report.
- This affidavit will be used by local law enforcement to create a police report (see Step 5).

Provide information about the crime at IdentityTheft.gov - this information will be used to create a personalized action plan, and the website can help to track progress, pre-fill forms and letters, and update the plan as needed.

STEP 5 – Report the Identity Theft to Law Enforcement

After receiving an identity theft report from the FTC, you may ask the local police department to create a police report documenting the identity theft allegation. Ask law enforcement for a copy of the report, if possible.

You will need to bring:

- the FTC Identity Theft Report;
- government identification;
- proof of address; and
- any other proof of the identity theft.

The combination of the police report and identity theft report will create a record that can be used with creditors, banks, credit reporting companies, and other financial institutions to officially corroborate that the identity theft has occurred.

After contacting the local police, you can also contact the following:

- District Attorney - Contact the local district attorney's Office.
- Attorney General - Contact the attorney general's consumer protection unit and the prosecution unit to report the fraud. Find contact information at www.naag.org
- Federal Law Enforcement - Contact the local FBI field office or submit an online tip at http://tips.fbi.gov. Look up the local field office at www.fbi.gov/contact-us/field.

STEP 6 – Consider Placing an Extended Fraud Alert and/or Credit Freeze

Once the identity theft report and police report are obtained, you may wish to request an extended fraud alert with the three credit reporting companies. This alert will require companies issuing credit in your name to verify that you are actually attempting to open a line of credit.

- Contact all three credit reporting companies separately.
- Use the identity theft report (the combination of the police report and FTC identity theft report) to create an extended fraud alert:
  - The extended fraud alert is free.
  - The extended fraud alert is good for seven years.
  - The extended fraud alert entitles you to two free credit reports from all three of the credit reporting companies within 12 months of placing the extended alert.
- If permitted in your state, consider placing a credit freeze on your credit report. A credit freeze prevents companies from checking someone's credit, making it more difficult for fraudsters to use your identity to obtain credit. A credit freeze will also affect your own ability to access credit (including legitimate lender and employer inquiries), so carefully consider if this option is right for you.

STEP 7 – Order Three Free Credit Reports

Once an extended fraud alert is created, you are entitled to free credit reports from each of the credit reporting companies.

To obtain your free credit reports:

- call all three credit reporting companies, inform them of the fraud alert, and request a free copy of your credit report; and
- ask each company to show only the last four digits of your Social Security number on the report.

STEP 8 – Contact the Internal Revenue Service

Even if you do not think the identity theft is related to your taxes, it is possible that your Social Security number could be used to file fraudulent tax returns. The IRS provides assistance in cases involving identity theft. You may need to submit an IRS Identity Theft Affadavit (Form 14039).

IRS Identity Protection Specialized Unit

(800) 908-4490

www.irs.gov/identitytheft

STEP 9 – Contact the Social Security Administration

If you suspect your Social Security number has been misused, call the Social Security Administration to report the misuse.

Social Security Administration Fraud Hotline

(800) 269-0271

(866) 501-2101 (TTY)

P.O. Box 17785

Baltimore, MD 21235

STEP 10 – Dispute Fraudulent Activity

If any of the perpetrator's fraudulent efforts were successful, you also will need to take the following steps, broken down by category:

Check Fraud/Bank Account Identity Theft

- Contact any financial institution where you have a checking or savings account or where your identity was used to fraudulently open such an account.

- Close these accounts, fraudulent or otherwise.
- Ask the bank to report the identity theft to check verification services.

Credit Card Identity Theft

- Carefully read account statements regularly to look for fraudulent charges.
- Contact relevant banks or credit card companies to dispute fraudulent charges.

Fraudulent Loan or Other Debt Identity Theft

- Contact the three credit reporting companies (Equifax, Experian, and Transunion—see Step 1) as well as the companies that issued the credit to dispute any fraudulent lines of credit in your name.
- Contact any debt collector for a fraudulent debt **within 30 days** of receiving notice.
- Use copies of the police report, identity theft affidavit, and any other documents to assist in this process (see Steps 4-5).
- Obtain copies of any documents used to apply for credit or make charges in your name.
- Contact the credit reporting companies and file a dispute about fraudulent activity on your credit report.

Medical Identity Theft

- Request from your health insurance company a list of benefits that were paid to date.
- Examine records from medical and pharmacy providers for accuracy and request corrections, as needed. If the request to review or correct your medical records is refused, file a complaint at the U.S. Department of Health and Human Services at www.hhs.gov/ocr/hipaa. Consumers have a right to correct their medical records.

Sample letters for contacting banks and other companies are available from the FTC at www.identitytheft.gov/sample-letters

ATTEND TO YOUR HEALTH

The toll of financial fraud may extend well beyond lost money.

FINRA Foundation research indicates that nearly **two-thirds of fraud victims experience at least one severe emotional consequence**—including stress, anxiety, insomnia, and depression.

If you are suffering in the aftermath of a financial crime, seek help. Many mental health professionals offer services on a sliding-fee scale.

STEP 11 – Consider Civil Remedies

Civil attorneys who work for victims of financial fraud can analyze the particular facts and circumstances of your case and counsel you on the available civil remedies. The National Crime Victim Bar Association can provide referrals to attorneys who litigate on behalf of victims of crime and who offer initial consultations at no cost or obligation.

National Crime Victim Bar Association

For a referral, email: attorneyreferrals@victimsofcrime.org

Find more information about civil justice at www.victimbar.org.

There are several potential civil options for victims of identity theft:

- Many states have laws that allow you to directly sue the identity thief.
- A business or organization that failed to properly secure your personal information may be held liable if the perpetrator used that information to steal your identity.
- Banks may be held liable for failing to prevent identity thieves from opening a checking account in your name.
- Under the Fair Credit Reporting Act, credit reporting agencies may be required to pay you damages for failing to add an identity theft annotation to your credit report.

Step 12 – Follow Up

Review the steps you've taken and follow up after 30 days with any law enforcement agencies or organizations that serve victims.

PREVENTION TIPS

Once your identity has been stolen, even if you have completed the steps above, you may be more susceptible to a compromised identity in the future.

Protect Yourself:

- Keep all personal and financial records in a locked storage device or in a password-protected electronic file.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you have initiated the contact or know the person who you are communicating with.
- Shred all paper with identifying information before disposing of it.
- Use caution at stand-alone ATM kiosks, gas pumps, and other places where credit cards are often swiped and skimmers could be used.

Check:

- Monitor bank and credit card accounts weekly.
- Regularly monitor your credit reports. A free copy from each of the three major credit reporting companies is available every 12 months through www.annualcreditreport.com.
- Review the information at www.safechecks.com to find out how to order safer checks.

Stop:

- When someone requests your Social Security number, ask if you can provide alternate information. At medical offices, use an identifier that is not your Social Security number.
- Be alert to impersonators. If a company, even one you have an account with, sends an email asking for personal information, don't click on any links. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement or the back of your credit/debit card. Ask whether the company really sent a request.
- Beware of phone calls that display "IRS" in the caller ID or a Washington, DC, area code. As tax scams increase, know that the IRS will first contact you by mail if they need to reach you. To verify correspondence, call the IRS directly at (800) 829-1040.
- Refer to www.consumer.ftc.gov/features/feature-0014-identity-theft for a complete list of prevention tips.